A Combinatorial Approach to Quantum Error Correcting Codes

German Luna, Samuel Reid, Bianca De Sanctis, Vlad Gheorghiu

Version of April 26, 2013

Abstract

Motivated from the theory of quantum error correcting codes, we investigate a combinatorial problem that involves a symmetric n-vertices colourable graph and a group of operations (colouring rules) on the graph: find the minimum sequence of operations that maps between two given graph colourings. We provide an explicit algorithm for computing the solution of our problem, which in turn is directly related to computing the distance (performance) of an underlying quantum error correcting code. Computing the distance of a quantum code is a highly non-trivial problem and our method may be of use in the construction of better codes.

1 Introduction

With the recent advances in quantum information processing, protecting a physical system from environmental noise became an ultimate desideratum in the construction of a large scale quantum computer. Quantum error correcting codes, introduced about a decade ago [1, 2], play an important role in this respect and allow the protection of fragile quantum computation against undesired errors via the use of redundancy.

An important class of quantum error correcting codes are the *stabilizer codes* [3], which are the quantum analog of classical linear codes [4]. Most known quantum error correcting codes belong to the class of stabilizer codes, which in turn are equivalent [5] to the so-called *graph codes*. The latter, as their name states, are codes built using an undirected symmetric graph on n vertices. For more details about their properties see [6, 7, 8].

The performance of quantum codes is characterized by the *distance* of the code, a positive integer that specifies how many errors the code tolerates (see e.g. [9] for a detailed discussion). The classical analog of the quantum distance is the well-known Hamming distance [4]. A vast amount of work has been dedicated to constructing quantum error correcting codes with the highest possible distance, see [10] for a list of up-to-date codes and bounds on the distance.

Given a quantum error correcting code, determining its distance is highly non-trivial and in general requires numerical methods. Inspired by this, in the current article we investigate a combinatorial problem involving graphs and operations on graphs, whose solution provides the distance of a corresponding graph code. Our solution is algorithmic and, although scales exponentially[1] with the number of vertices of the graph, can nevertheless be of great use in the construction of quantum error correcting codes. The solution we provide is elegantly described by linear systems over finite

---

[1]Up to our current knowledge, determining the distance of a quantum code seems to be a computationally-hard problem.

fields with the properties of the solution space providing the distance of the code. Although the space of solutions itself can be compactly described using a suitable basis, computing the distance reduces to searching among *all* possible solutions, and is this searching that makes the problem exponentially-hard.

Even though the problem we investigate is motivated from the theory of quantum error correcting codes, we believe, given its combinatorial nature, that it may be of intrinsic interest to the discrete mathematics community, see e.g. [11] for a related work.

2 Graph Labellings and Diagonal Distance

Let $G_n = (V, E)$ be a graph with n vertices where V is the vertex set of G_n and E is the edge set of G_n. A graph labelling of G_n is a function $L : V \to \mathbb{Z}/2\mathbb{Z}$, which can be written as an element of $(\mathbb{Z}/2\mathbb{Z})^n$ by using the ordering of the vertices. For example, if we have a graph with $V = \{v_1, v_2, v_3, v_4, v_5\}$ and a graph labelling $L = \{(v_1, 0), (v_2, 1), (v_3, 0), (v_4, 0), (v_5, 1)\}$, then we write the graph labelling simply as $(0, 1, 0, 0, 1) \in (\mathbb{Z}/2\mathbb{Z})^5$ by requiring that the ith entry in the element of $(\mathbb{Z}/2\mathbb{Z})^5$ is the label of the ith vertex of the graph for $1 \leq i \leq 5$. In order to simplify notation we will henceforth refer to the graph labelling L as the element of $(\mathbb{Z}/2\mathbb{Z})^n$ instead of as the function $L : V \to (\mathbb{Z}/2\mathbb{Z})^n$. In order to define the diagonal distance of a graph G_n we need to define two operations which indicate the possible ways to move between graph labellings. Defining these operations requires the notion of the adjacency matrix Γ of a graph G_n which is defined as the $n \times n$ matrix with $\Gamma_{ij} = 1$ if $(v_i, v_j) \in E$ (there is an edge between v_i and v_j) and $\Gamma_{ij} = 0$ if $(v_i, v_j) \notin E$ (there is no edge between v_i and v_j). Observe that $(\mathbb{Z}/2\mathbb{Z})^n$ is the set of all graph labellings of a graph with n vertices and so our operations our defined as follows.

Definition 1. *Define two operations applied to the graph labelling L of G_n for arbitrary $v_i \in V$ by,*

- $Z_i : (\mathbb{Z}/2\mathbb{Z})^n \to (\mathbb{Z}/2\mathbb{Z})^n$ *defined by* $L_i \mapsto L_i + 1 \mod 2$.

- $X_i : (\mathbb{Z}/2\mathbb{Z})^n \to (\mathbb{Z}/2\mathbb{Z})^n$ *defined by* $L_j \mapsto L_j + \Gamma_{ij} \mod 2, \forall 1 \leq j \leq n$.

where L_i denotes the ith entry in L.
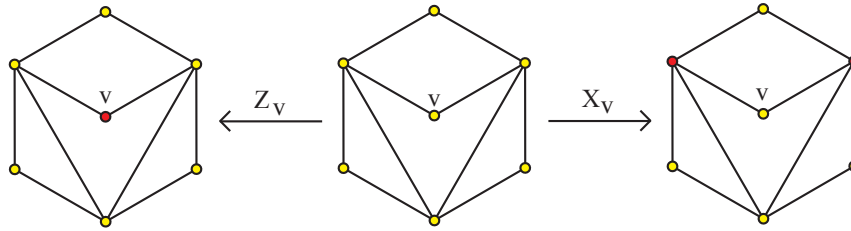

Figure 1: An example of the two operations over $(\mathbb{Z}/2\mathbb{Z})^n$ applied to a graph with 7 vertices.

We name an element in the group of operations at the ith vertex of G_n by $O_i \in \langle Z_i, X_i \rangle$; that is, O_i is an arbitrary element of the group of operations generated by the operations Z_i and X_i with composition of maps as the group operation. The characteristic η-function is defined by,

$$\eta(O_i) = \begin{cases} 1 & \text{if } O_i \neq I \\ 0 & \text{if } O_i = I \end{cases} \tag{1}$$

where $I : (\mathbb{Z}/2\mathbb{Z})^n \to (\mathbb{Z}/2\mathbb{Z})^n$ is the identity map. We are now prepared to define the diagonal distance of a graph. Intuitively, the diagonal distance of a graph G_n is the minimum number of composed O_i's that change the labelling L of G_n to a non-zero number of other labellings before returning to the original labelling L. Formally, summing the characteristic η-function over a collection of O_i's counts the number of composed O_i's different from the identity. By ensuring that the composition (denoted by $\prod$) of the O_i's equals the identity map I, we guarantee that the graph returns to its original labelling. Notice that the diagonal distance is invariant under different numberings of the vertices, as long as the notation remains consistent throughout the usage of this algorithm.

Definition 2. *The diagonal distance $\Delta(G_n)$ of a graph G_n is defined as,*

$$\Delta(G_n) = \min \left\{ \sum_{i=1}^{n} \eta(O_i) > 0 \,\middle|\, \prod_{i=1}^{n} O_i = I, O_i \in \langle Z_i, X_i \rangle, 1 \leq i \leq n \right\} \tag{2}$$

3   Computing Diagonal Distance Over $\mathbb{Z}/2\mathbb{Z}$

Given a graph G_n, we construct the $n \times 2n$ matrix Λ by concatenating I_n and Γ as,

$$\Lambda = [I_n \mid \Gamma] \tag{3}$$

where I_n is the $n \times n$ identity matrix and Γ is the adjacency matrix of G_n. We think of I_n as the part of Λ which keeps track of Z_i applied to G_n and Γ as the part of Λ which keeps track of X_i applied to G_n. Let k^T be an arbitrary nonzero $1 \times 2n$ vector with entries in $\mathbb{Z}/2\mathbb{Z}$ and write

$$k^T = [k_1 \cdots k_n \mid k_{n+1} \cdots k_{2n}] \tag{4}$$

If $\Lambda k = 0 \pmod 2$, that is, if k is in the nullspace of Λ over $\mathbb{Z}/2\mathbb{Z}$, then we claim that k contains the information about the application of O_i's to G_n which changes the labelling L of G_n to a non-zero number of other labellings before returning to the original labelling L. In order to justify this claim we require the characteristic χ-function defined for $1 \leq i \leq n$ by

$$\chi(k_i) = \begin{cases} 1 & \text{if } k_i \neq 0 \text{ or } k_{i+n} \neq 0 \\ 0 & \text{if } k_i = k_{i+n} = 0 \end{cases} \tag{5}$$

By relating the characteristic χ-function and the characteristic η-function to each other we can relate elements $O_i \in \langle Z_i, X_i \rangle$ to a vector k that is constructed to encode the information in O_i. More precisely, we consider an arbitrary set of group operations $\{O_i\}_{1 \leq i \leq n}$ and for each $O_i = Z_i^{z_i} X_i^{x_i}$ construct the vector k with the ith entry given by $k_i = z_i \pmod 2$ and the $(i+n)^{\text{th}}$ entry given by $k_{i+n} = x_i \pmod 2$, where $1 \leq i \leq n$.

Lemma 1. *Let $\{O_i\}_{i=1}^{n}$ be an arbitrary collection of $O_i \in \langle Z_i, Xi \rangle$. Then for any O_i in this collection, there exists $z_i, x_i \in \mathbb{Z}/2\mathbb{Z}$ such that $O_i = Z_i^{z_i} X_i^{x_i}$ and*

$$\eta(O_i) = \chi(k_i) \tag{6}$$

where k is the $2n \times 1$ vector with $k_i = z_i$ and $k_{i+n} = x_i$ for $1 \leq i \leq n$.

Proof. Let $O_i = Z_i^{z_i} X_i^{x_i}$, where $z_i, x_i \in \mathbb{Z}$. Note that since labellings are elements of $\mathbb{Z}/2\mathbb{Z}$, then $Z_i^2 = I$ and $X_i^2 = I$ since these maps act by adding the same quantity twice. Thus $Z_i^{z_i} X_i^{x_i} = Z_i^{z_i \mod 2} X_i^{x_i \mod 2}$ and so O_i is equivalent to $Z_i^z X_i^x$ for some $x, z \in \mathbb{Z}/2\mathbb{Z}$. Construct the vector k as stated in the lemma. If $\eta(O_i) = 1$, then $Z_i^z X_i^x \neq I$ and so either $z \neq 0$ or $x \neq 0$, which implies that $\chi(k_i) = 1$. If $\eta(O_i) = 0$, then $Z_i^z X_i^x = I$ and so $z = x = 0$, which implies that $\chi(k_i) = 0$. Therefore, $\eta(O_i) = \chi(k_i)$. $\qquad\square$

We now prove another lemma which restricts the possible vectors k, and thus the possible set of group operations $\{O_i\}_{1 \leq i \leq n}$, which can satisfy the definition of diagonal distance.

Lemma 2. *Let $\{O_i\}_{1 \leq i \leq n}$ be a set of group operations with each $O_i = Z_i^{z_i} X_i^{x_i}$, where $z_i, x_i \in \mathbb{Z}/2\mathbb{Z}$. Then,*

$$\prod_{i=1}^n O_i = I \iff k \in \ker(\Lambda)/2\mathbb{Z} \tag{7}$$

where k is the $2n \times 1$ vector with $k_i = z_i$ and $k_{i+n} = x_i$ for $1 \leq i \leq n$.

Proof. Write a labelling $L \in \left(\mathbb{Z}/2\mathbb{Z}\right)^n$ of a graph G_n as an $n \times 1$ vector and represent $\langle Z_i, X_i \rangle$ by additive matrix operations as $Z_i(L) \cong L + e_i \mod 2$ and $X_i(L) \cong L + \text{col}_i(\Gamma) \mod 2$, where e_i is the $n \times 1$ matrix with 1 in the ith entry and 0 elsewhere and where $\text{col}_i(\Gamma)$ is the ith column of Γ. ($\Rightarrow$) Then for an arbitrary $O_i = Z_i^{z_i} X_i^{x_i}$ we have that O_i can be represented by an action on the labelling L as $O_i \cong L + z_i e_i + x_i \text{col}_i(\Gamma) \mod 2$. Then for any set of group operations $\{O_i\}_{1 \leq i \leq n}$,

$$\prod_{i=1}^n O_i \cong L + \sum_{i=1}^n z_i e_i + \sum_{i=1}^n x_i \text{col}_i(\Gamma) \mod 2 = L + \Lambda k \mod 2, \tag{8}$$

If $\prod_{i=1}^n O_i = I$, then $\prod_{i=1}^n O_i \cong L \mod 2$ which yields

$$L + \Lambda k = L \mod 2 \tag{9}$$

and therefore every set of group operations $\{O_i\}_{1 \leq i \leq n}$ has a representation as a vector in the kernel of Λ.

($\Leftarrow$) The backward implication follows from rewriting the previous equation, since we now assume that k is some arbitrary vector in the kernel. Use Lemma 1 to construct a set of group operations corresponding to k. Since $k \in \ker(\Lambda)/2\mathbb{Z}$ by assumption, we get that

$$L + \Lambda k = L \mod 2$$

Then, as in the other direction, we have that $\prod_{i=1}^n O_i \cong L$, which implies that $\prod_{i=1}^n O_i = I$. Therefore,

$$k \in \ker(\Lambda)/2\mathbb{Z} \iff \prod_{i=1}^n O_i = I. \tag{10}$$

$\qquad\square$

This leads to the main theorem regarding the computation of diagonal distance.

Theorem 1. *The diagonal distance $\Delta(G_n)$ of a graph G_n can be computed as*

$$\Delta(G_n) = \min\left\{ \sum_{i=1}^n \chi(k_i) > 0 \;\middle|\; k \in \ker(\Lambda)/2\mathbb{Z} \right\}. \tag{11}$$

4

Proof. By Lemma 1 and Lemma 2 we have that,

$$\Delta(G_n) = \min\left\{\sum_{i=1}^{n} \eta(O_i) > 0 \;\Big|\; \prod_{i=1}^{n} O_i = I, O_i \in \langle Z_i, X_i \rangle, 1 \le i \le n\right\}$$

$$= \min\left\{\sum_{i=1}^{n} \chi(k_i) > 0 \;\Big|\; k \in \ker(\Lambda)/2\mathbb{Z}\right\}. \tag{12}$$

$\square$

An immediate consequence of this theorem is a deterministic algorithm for computing the diagonal distance $\Delta(G_n)$ of any graph G_n. To run this algorithm, one must first compute a basis for $\ker(\Lambda)/2\mathbb{Z}$. Then the entire kernel must be spanned to check each vector k for $\chi(k)$, and the smallest $\chi(k)$ (along with its corresponding vector, if extra information is desired) is stored. Once the algorithm terminates, the smallest of all the $\chi(k)$s will have been stored and will be equal to the diagonal distance $\Delta(G_n)$.

4   Generalization of Diagonal Distance to Multigraphs over $\mathbb{Z}/p\mathbb{Z}$

We now generalize the diagonal distance of a graph over $\mathbb{Z}/2\mathbb{Z}$ to the diagonal distance of a multigraph (a graph that can have multiple edges between vertices) over $\mathbb{Z}/p\mathbb{Z}$, where p is prime. We define a graph labelling exactly as over $\mathbb{Z}/2\mathbb{Z}$ and note that the set of all graph labellings is now $(\mathbb{Z}/p\mathbb{Z})^n$. The operations Z_i and X_i applied to a graph labelling is defined exactly as over $\mathbb{Z}/2\mathbb{Z}$, except the adjacency matrix Γ of a multigraph G_n is defined as the $n \times n$ matrix with $\Gamma_{ij} = k$ if there are k occurrences of $(v_i, v_j) \in E$ (there are k edges between v_i and v_j) and $\Gamma_{ij} = 0$ if $(v_i, v_j) \notin E$ (there is no edge between v_i and v_j). We can then define the group of operations
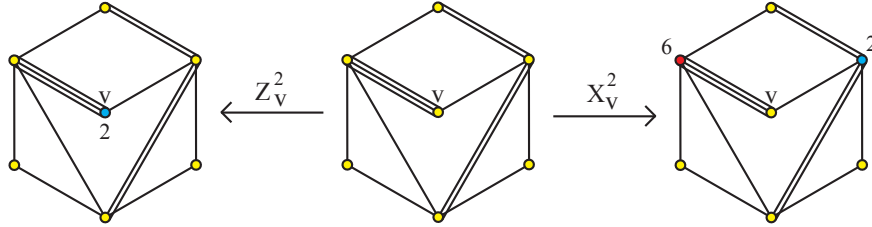

Figure 2: An example of the two operations Z_i^2 and X_i^2 applied to a multigraph with 7 vertices.

$O_i = \langle Z_i, X_i \rangle$, with our operations defined over $\mathbb{Z}/p\mathbb{Z}$ in order to obtain the straightforward generalization of Theorem 1 to $\mathbb{Z}/p\mathbb{Z}$ by writing mod p everywhere that mod 2 is written in the proofs of Lemma 1, Lemma 2, and Theorem 1.

Theorem 2. *The diagonal distance $\Delta(G_n)$ of a graph G_n can be computed as,*

$$\Delta(G_n) = \min\left\{\sum_{i=1}^{n} \chi(k_i) > 0 \;\Big|\; k \in \ker(\Lambda)/p\mathbb{Z}\right\}. \tag{13}$$

5

5 Minimal Diagonal Distance of Codes Over $\mathbb{Z}/p\mathbb{Z}$

Thus far we have considered the diagonal distance $\Delta(G_n)$ over $\mathbb{Z}/2\mathbb{Z}$ of a graph G_n and, more generally, the diagonal distance $\Delta(G_n)$ over $\mathbb{Z}/p\mathbb{Z}$ of a multigraph G_n. In either of these cases, we built into the definition of diagonal distance that $\prod_{i=1}^{n} O_i = I$ where $I : (\mathbb{Z}/p\mathbb{Z})^n \to (\mathbb{Z}/p\mathbb{Z})^n$ is the identity map. Yet, we can extend this notion to requiring that $\prod_{i=1}^{n} O_i = L$, where $L : (\mathbb{Z}/p\mathbb{Z})^n \to (\mathbb{Z}/p\mathbb{Z})^n$ is some specific map, e.g. the map sending the configuration $\vec{0}$ to $\vec{1}$.

Let $\{C_1, ..., C_k\}$ be a set of graph labellings (i.e. codewords), where $C_1 = \vec{0}$. We then want to determine the diagonal distance between any two graph labellings C_r and C_s in this set, the distance of the code, which can be defined as follows.

Definition 3. *For a multigraph G_n and a set of graph labellings $\{C_1, C_2, ..., C_k\}$, the diagonal distance $\Delta_{rs}(G_n)$ between two graph labellings C_r and C_s is defined as,*

$$\Delta_{rs}(G_n) = \min\left\{\sum_{i=1}^{n} \eta(O_i) > 0 \;\middle|\; \prod_{i=1}^{n} O_i = L_{rs}, O_i \in \langle Z_i, X_i \rangle, 1 \leq i \leq n\right\} \tag{14}$$

where G_n is assumed to be originally labelled by C_r and L_{rs} is the map sending the graph labelling C_r to the labelling C_s.

Similarly to computing $\Delta(G_n)$, we can minimize $\Delta_{rs}(G_n)$ by minimizing the summation of the characteristic χ-function of vector k' such that $\Lambda k' = C_r - C_s \mod p$. It is a straightforward generalization of Lemma 1 and Lemma 2 in order to obtain the analogue of Theorem 2 for distance of a code.

Theorem 3. *The generalized diagonal distance $\Delta_{rs}(G_n)$ of a graph G_n can be computed as,*

$$\Delta_{rs}(G_n) = \min\left\{\sum_{i=1}^{n} \chi(k'_i) > 0 \;\middle|\; \Lambda k' = C_r - C_s \mod p\right\} \tag{15}$$

where G_n is originally labelled by C_r.

Note that the distance δ of a code $\{C_1, C_2, ..., C_k\}$ is simply $\min\{\Delta_{rs}(G_n) \mid r, s \in \{1, 2, ...k\}\}$

6 Computational Example

We run the main algorithm on the 5-cycle graph in $\mathbb{Z}/2\mathbb{Z}$. It is well-known that the diagonal distance of the 5-cycle is 3, for example by the set of operations shown in Figure 3. This can be found directly using our algorithm. To compute the diagonal distance, we must first set up the matrix $\Lambda = [I_n \mid \Gamma]$. For the 5-cycle, this is a 5×10 matrix which has many possibilities depending on how the vertices are numbered. However, diagonal distance is invariant under different numberings and so we will just pick one.

$$\Lambda = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \end{bmatrix}$$
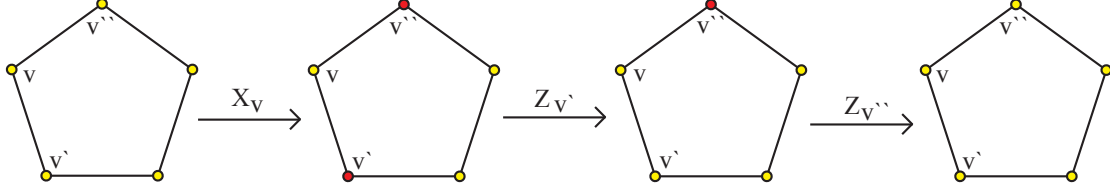
Figure 3: An example of three operations that illustrate the diagonal distance of the 5-cycle.

Next we must compute the kernel of this matrix. Some computation gives that the kernel has the following basis vectors.

$$k_1 = (0, 1, 0, 0, 1, 1, 0, 0, 0, 0)^T$$
$$k_2 = (1, 0, 1, 0, 0, 0, 1, 0, 0, 0)^T$$
$$k_3 = (0, 1, 0, 1, 0, 0, 0, 1, 0, 0)^T$$
$$k_4 = (0, 0, 1, 0, 1, 0, 0, 0, 1, 0)^T$$
$$k_5 = (1, 0, 0, 1, 0, 0, 0, 0, 0, 1)^T$$

To find the vector in the kernel with the least amount of 1's in it, we must search through all the linear combinations of these basis vectors. It is easy enough to write a program to do this. For this example, it actually turns out that the linear combinations with the least amount of 1's in them are exactly the basis vectors themselves. Notice that all of these vectors have 3 1's in them. Therefore, the diagonal distance of the 5-cycle graph is 3.

Acknowledgments

References

[1] Peter W. Shor. Scheme for reducing decoherence in quantum computer memory. *Phys. Rev. A*, 52(4):R2493–R2496, 1995.

[2] A. R. Calderbank and Peter W. Shor. Good quantum error-correcting codes exist. *Phys. Rev. A*, 54(2):1098–1105, 1996.

[3] Daniel Gottesman. Stabilizer codes and quantum error correction. e-print arXiv:quant-ph/9705052.

[4] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes*. North-Holland Mathematical Library, Amsterdam, 1977.

[5] Dirk Schlingemann. Stabilizer codes can be realized as graph codes. e-print arXiv:quant-ph/0111080.

[6] M. Hein, W. Dur, J. Eisert, R. Raussendorf, M. Van den Nest, and H. J. Briegel. Entanglement in graph states and its applications. e-print arXiv:quant-ph/0602096.

[7] Shiang Yong Looi, Li Yu, Vlad Gheorghiu, and Robert B. Griffiths. Quantum-error-correcting codes using qudit graph states. *Phys. Rev. A*, 78(4):042303, 2008.

[8] Sixia Yu, Qing Chen, and C.H. Oh. Graphical quantum error-correcting codes. e-print arXiv:0709.1780 [quant-ph].

[9] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information.* Cambridge University Press, Cambridge, 5th edition, 2000.

[10] Markus Grassl. Bounds on the minimum distance of linear codes. Online available at http://www.codetables.de, 2007.

[11] T. Bohman, A. Dudek, A. Frieze, and O. Pikhurko. Flips in graphs. *SIAM Journal on Discrete Mathematics*, 24(3):1046–1055, 2010.

German Luna
Department of Mathematics and Statistics, University of Calgary, Calgary AB T2N 1N4, Canada
E-mail: galunapa@ucalgary.ca

Samuel Reid
Department of Mathematics and Statistics, University of Calgary, Calgary AB T2N 1N4, Canada
E-mail: smrei@ucalgary.ca

Bianca De Sanctis
Department of Mathematics and Statistics, University of Calgary, Calgary AB T2N 1N4, Canada
E-mail: bddesanc@ucalgary.ca

Vlad Gheorghiu
Department of Mathematics and Statistics, University of Calgary, Calgary AB T2N 1N4, Canada
Institute for Quantum Science and Technology, Calgary AB T2N 1N4, Canada
E-mail: vgheorgh@ucalgary.ca